Grave new world: mass surveillance and labour rights

by Liam Welch

Picture: istock

Science fiction has always warned us that with technology comes the looming potential for mass monitoring and encroachment into our personal lives. George Orwell had Big Brother and the telescreen, monitoring everyone from their homes. Philip K Dick thought up the authoritarian 'Precogs', spotting offences before they had already happened. **>>>**

“Workers are increasingly being surveilled, profiled, supervised and assessed by various methods that would have been unthinkable 15 years ago. A worker’s whereabouts can be tracked through access cards, vehicle trackers and company mobile phones. Using keystroke technology, employers can monitor every single action taken on a company computer or device.”

>>> More recently, Charlie Brooker gave us ‘Arkangel’, an implanted microchip technology used to track children. Worryingly, instead of viewing these fictional technologies as a warning, employers increasingly appear to be using them as inspiration.

Data use in the workplace

It is now common for job applicants’ online history and social media to be trawled before interviews. This raises real privacy considerations, especially given that young people entering the workplace today will not remember a world where social media did not exist. Such trawls are also routinely used as evidence by employers in disciplinary proceedings.

Furthermore, people’s data can be bought by potential employers from third-party data brokers. Specialist worker assessment software can then be used to create psychological profiles of candidates. Using this software, a candidate’s geographic location, social media history, personal and professional relationships, and their consumer choices can all be screened. During the selection process itself, technologies such as HireVue claim to assess candidates’ suitability jobs by using algorithms based on video footage to score applicants. The footage is then used to analyse numerous factors (‘data points’), which include workers’ verbal responses, their intonation, and non-verbal communication (ie body language) to allegedly predict future job performance.

It comes as no surprise, then, that workforce data is being used in a number of monitoring contexts. Workers are increasingly being surveilled, profiled, supervised and assessed by various methods that would have been unthinkable 15 years ago. A worker’s whereabouts can be tracked through access cards, vehicle trackers and company mobile phones. Using keystroke technology, employers can monitor every single action taken on a company computer or device. Workers are also often monitored in the workplace via CCTV, and have little real control over how a company handles or retains that data. Workers know that footage could easily be obtained and used against them, but at the same time there is little guarantee that information could be promptly obtained should it be potentially useful to them against their employer.

With the fast pace of modern technological advance come further intrusions into workers’ private lives. In the criminal justice system electronic tags have been used since the 1990s to ensure compliance with remand and license conditions. But now employers are starting to ‘provide’ such ‘wearable tech’ to workers. In 2016 it was reported that Amazon applied for two patents for wristbands that monitor the locations of workers’ hands in relation to their inventory bins, in order to monitor their performance. Amazon has form: for a long time its workers have been continuously tracked in warehouses. Workers are expected to carry personal satellite navigation computers that dictate the route that they are expected to take around the warehouse to shelve goods, and that then measure whether they meet targets. This data is used to set further targets, which can result in dismissal

should the workers fail to meet them. These practices have been said to lower worker wellbeing, and to lead to workplace injuries as workers rush to meet targets.

In 2018 West Virginia teachers were forced to take strike action over proposed changes to their public worker health plan, which required them to download a points based fitness tracker app designed to monitor the users' biometric data, including steps taken and their heartrate. Those who declined to comply, or who did comply but failed to rack up enough points, faced a compulsory penalty of $500 per year. The proposals may have been defeated through industrial action, but the spectre looms large.

It isn't such a leap for employers to begin monitoring our sleep, our activity levels and our movements, with penalties for perceived inefficiency. In the non-unionised hinterlands of today's economy, what is to stop employers insisting on workers wearing such monitoring devices around the clock?

This assumes that workers are left with the option of removing their monitoring devices. Drawing on experiences tracking household pets, tech firms offering microchip implants are already in talks with businesses in the UK to microchip their staff. This already appears to be in place in firms in the USA and Sweden. In 2017 the Wisconsin-based company Three Square Market announced that it would be offering to implant 'identification chips' into the hands of its workers, on an ostensibly voluntary basis. The chips are injected between the thumb and forefinger where they can be used to gain access to security doors, log in to company computers and photocopiers, and operate staff vending machines. Aside from the obvious corporal, human rights and privacy issues that this raises, there are very real health concerns. Since the 1990s studies have shown evidence that microchips can cause cancerous tumours to develop in rats and mice near the implantation site. Whilst Three Square Market reported that initial take up was good, given the current inequality of arms in most worker/employer relationships, can such decisions ever be genuinely voluntary and allow for true and informed consent?

Tracking devices contribute data to 'people analytics' and, unsurprisingly, this phenomenon bleeds into areas such as recruitment, disciplinary investigations and productivity. This raises issues of workers' rights to challenge what data is kept, how it is used and stored, and when it will be destroyed. These are important questions in any event, but will be especially pressing should biometric data harvesting and microchip implantations gain a real foothold. Leaks and hacks are prevalent in today's society, and there is a worrying commodification of date. It seems unlikely that employers could say with any confidence that such intimate data would be sufficiently secure. **>>>**

>>> The next steps for employers

On the basis of the technology already in place to assess job applicants, a natural extension for employers is to then use these analytics to assess how a worker will continue to perform in a role. This could lead to health data being used to predict and dismiss workers before they develop health conditions. Predictions could also be made based on a worker's behaviour in order to dismiss them in relation to their anticipated future conduct, before reaching the two-year continuous service requirement for bringing an unfair dismissal claim. Given the obviously anti-union stance of many of the big tech and gig-economy employers, this could also be used against workers who may show potential as trade union organisers and representatives.

Workers' data rights

Workers do have some existing rights that they should be aware of when it comes to data. The General Data Protection Regulations (GDPR) allow workers the right to know what data an employer collects and how they intend to use it. Employers must also use 'privacy notices' to explain how data is going to be handled, and these should be displayed and made available to workers. Employers cannot collect data indiscriminately and must have a lawful ground for the processing of data, and workers can challenge this if they think it is unlawful. But consent is not normally needed in the employment context, so there is no opt-out of the GDPR for employees. Workers should bear in mind that the Information Commissioner's Office have the power to issue sanctions for employers for non-compliance with the regulations, and should they suspect irregularity they should not hesitate to contact their trade union and/or the ICO.

Furthermore, GDPR provides that workers should not be subject to solely automated decisions if that have a potentially significant effect. Should an employer wish to use fully automated processing and profiling, they must carry out a privacy impact assessment, and consult the ICO for guidance if there is a high risk to rights and freedoms. In reality it remains to be seen how easy it will be for employers to skirt these provisions.

In the legal context, individuals have a right to a private life and correspondence under Article 8 of the European Convention on Human Rights, and this is also extended to the workplace, albeit in a restricted manner. In the case of *Bărbulescu v Romania*, which was escalated to the European Court of Human Rights (ECHR), it was found that the right to a private social life in the workplace could not be reduced to zero and that it should be respected, although could be restricted as far as necessary. This means that whilst an employer can place

"The General Data Protection Regulations allow workers the right to know what data an employer collects and how they intend to use it. Employers must use 'privacy notices' to explain how data is to be handled, and these should be displayed and made available to workers. Employers cannot collect data indiscriminately and must have a lawful ground for the processing of data, and workers can challenge this."

limits on a workers use of communications and social media whilst at work, they cannot be restricted completely. On the other hand, the recent ECHR case of *López Ribalda and Others v Spain* found that employers did not breach their employees human rights in covertly recording workers via CCTV. This was justified on the basis of a reasonable suspicion of serious misconduct on the part of the employees, and the potential for significant losses as a result. The ECHR did accept however that a simple, slight suspicion of employee wrongdoing would not justify the installation of covert video surveillance by an employer. Therefore covert video surveillance by employers is potentially permissible, but only if the employer has sufficient justification.

Despite the importance of the issues raised above, perhaps unsurprisingly the current Tory administration do not appear to be putting measures in place to tackle these encroachments and both the government's recently announced Artificial Intelligence Council and its Centre for Data Ethics and Innovation have failed to solicit or include any representation from workers. Whilst the Trades Union Congress are fully aware of the disquieting trends detailed above; it remains crucial that workers report the current practices of their employers to their trade union. It is particularly important that any proposals for implementation of new policies and practices are disclosed as soon as possible to ensure that their union is fully abreast of developments. Under the Trade Union and Labour Relations (Consolidation) Act employers are under a legal obligation to disclose material information to trade unions for the purposes of all stages of collective bargaining, which should be engaged in in the unionised workplace prior to the alteration of workers' terms and conditions. Workers and unions should be vigilant that employers do not attempt to circumvent this when implementing new data-driven policies.

Should workers have concerns that their employer is currently breaching their data rights through monitoring practices, or suspect that they have been subject to autonomous decision making then this should be reported to the ICO as well as to their trade union as soon as possible. Similarly, if a worker feels that their employer is excessively limiting their social communications or surveilling them without sufficient justification whilst at work, then they should ensure that this is reported to their trade union and they should seek legal advice.

Another dystopian science fiction writer, William Gibson, once said "the future has arrived – it's just not evenly distributed yet". Employers have leapt on new technology, and this is a crucial time for workers to be vigilant: workers and unions must take a role in the development of how emerging technologies are applied and regulated. The alternative is to allow for further encroachment into workers' personal lives and a deterioration of working conditions, which must not be allowed to happen in any version of the future.

Liam Welch is a solicitor at the National Union of Rail, Maritime and Transport Workers (RMT) union. He is writing in a personal capacity.